Robert A. Agresta, Esq. (RA0218)
THE AGRESTA FIRM, P.C.
24 Grand Avenue
Englewood, New Jersey 07631
(201) 399-6888
robert.agresta@agrestalaw.com
Attorneys for Columbus LTACH, LLC

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY

COLUMBUS LTACH, LLC d/b/a SILVER LAKE HOSPITAL *Plaintiff,* v. OPTUM, INC., CHANGE HEALTHCARE INC. ABC Corps. 1-100; *Defendants.*	CIVIL ACTION Case No.: JURY TRIAL DEMANDED

Plaintiff Columbus LTACH, LLC d/b/a Silver Lake Hospital ("Silver Lake") brings this Complaint against Defendants Optum, Inc. ("Optum"), and Change Healthcare Inc. ("Change") (collectively, "Defendants") based upon its personal knowledge, investigation by counsel, and review of public documents and states as follows:

INTRODUCTION

1. Columbus brings this action for Defendants' failure to timely and adequately process and pay the amounts due for their medical services and for negligence resulting in the Columbus' inability to admit patients.

2. Change is a healthcare company that provides payment and revenue cycle services, clinical and imaging services, and other services to its clients. It is a lynchpin of a system which facilitates the payment of approximately $100 million per day to health care providers, such as hospitals, many of which have limited liquidity.

3. According to the Wall Street Journal, "Change processes around 15 billion transactions a year."[1]

4. Columbus seeks to hold Defendants responsible for the harms caused and will continue to cause the Columbus in the massive and preventable cyberattack purportedly discovered by Defendants on February 21, 2024, in which cybercriminals, known as the BlackCat/ALPHV ransomware group, infiltrated Defendants' inadequately protected network and accessed highly sensitive information which was being kept unprotected ("Data Breach").

5. According to the Wall Street Journal, "The hackers who attacked UnitedHealth Group's Change Healthcare unit were in the company's networks for more than a week before they launched a ransomware strike." *See* https://www.wsj.com/articles/change-healthcare- hackers-broke-in-nine-days-before-ransomware-attack-7119fdc6 ("Between Feb. 12 and when the ransomware was detonated on Feb. 21, the hackers were moving laterally within Change's network").

6. Indeed, Columbus was wholly unaware of the Data Breach until they were unable to access important and sensitive information.

7. As a result of the breach, Change "disconnected [its] systems to prevent further impact," according to its statement released on February 26, 2024. With those

[1] [1] https://www.wsj.com/articles/change-healthcare-hackers-broke-in-nine-days-before-ransomware-attack- 7119fdc6

systems disconnected, Columbus was cut off from over 100 services provided by Change, including benefits verification, claims submission, and prior authorization. Without those services, Columbus could not be admit, discharge or be paid for its work with patients.

8. Defendants disregarded the rights of Columbus by intentionally, willfully, recklessly, and/or negligently failing to take and implement adequate and reasonable measures to ensure that sensitive information was safeguarded and failing to take available steps to prevent unauthorized disclosure of data and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. Defendants further harmed Columbus by intentionally, willfully, recklessly, and/or negligently implementing procedures to disconnect the services that they rely on to secure payment and to admit patients from other discharging facilities. Columbus are entitled to injunctive and other equitable relief.

PARTIES, JURISDICTION, AND VENUE

9. Plaintiff Columbus LTACH, LLC is a corporate citizen of New Jersey. It is a New Jersey limited liability company that maintains its principal place of business and corporate headquarters in Newark, New Jersey. It operates the following two units in a single facility encompassing 63 beds of Long Term Acute Care and 62 beds for co-occurring substance use disorder and psychiatric conditions. These locations comprise the "Columbus."

10. Defendant Optum, Inc. ("Optum") is a corporate citizen of Minnesota. It is a corporation with a principal place of business located at 11000 Optum Circle, Eden Prairie, Minnesota 55344. Optum is a subsidiary of United Healthcare, Inc.

11. Defendant Change Healthcare Inc. ("Change") is a corporate citizen of

Tennessee. It is a corporation with a principal place of business located at 424 Church Street, Suite 1400, Nashville, Tennessee 37219. Change is a subsidiary of Optum.

12. This Court has subject matter jurisdiction as complete diversity exists amongst the parties under 28 U.S.C. §1332(a)(1). Plaintiff is a New Jersey limited liability company with a principal place of business in New Jersey. Optum is a Minnesota corporation with its headquarters in Minnesota. Change is a Tennessee corporation with its headquarters in Tennesse.

13. The amount in controversy, exclusive of interests and costs, exceeds $75,000.00.

14. Venue in the District of New Jersey is proper pursuant to 28 U.S.C. §1391(b)(3), as plaintiff resides in the district.

15. Supplemental jurisdiction to adjudicate issues pertaining to state law is proper in this Court under 28 U.S.C. § 1367.

16. Venue is proper in this Court under 28 U.S.C. § 1391 because a substantial part of the events that gave rise to Columbus' claims took place within this District and Defendants conduct business in this Judicial District.

17. This matter should be transferred to the District of Minnesota and joined to MDL 3108 now pending in that district.

FACTUAL ALLEGATIONS

18. On February 21, 2024, Change failed to prevent a cyberattack affecting a number of its systems and services (the "Data Breach"). At 4:27 PM EST, it announced that it was "experiencing a network interruption related to a cyber security issue," that it had disconnected its systems, and that disruption to its services was expected to last at

least through the day.

19. According to the Wall Street Journal, "The hackers who attacked UnitedHealth Group's Change Healthcare unit were in the company's networks for more than a week before they launched a ransomware strike." *See* https://www.wsj.com/articles/change-healthcare- hackers-broke-in-nine-days-before-ransomware-attack-7119fdc6 ("Between Feb. 12 and when the ransomware was detonated on Feb. 21, the hackers were moving laterally within Change's network … The length of time the attackers were in the network suggests they might have been able to steal significant amounts of data from Change's systems.")

20. As a result of Change's failures, hospitals, and other medical providers, including Columbus, have been unable to receive payment for their services and to discharge and bill patients which is critical to Columbus' admitting programs. Columbus, like most hospitals operates with limited liquidity and this disruption threatened and continues to threaten to bankrupt hundreds if not thousands of care providers if it hasn't done so already.

21. Change is a health software services company which provides payment and revenue cycle services, clinical imaging services, and other services to its clients. It is a large player in the healthcare sector, as its services allow health care providers to resolve payments for their care. It handles 15 billion healthcare transactions totaling more than $1.5 trillion annually. According to the Department of Justice, it handles 50 percent of all medical claims in the United States.

22. Columbus is a medical provider which suffered delays in processing claims and revenue cycle services as a result of the Data Breach as well as an inability to

admit patients due to Columbus' inability to obtain prior authorization for patient admissions as Columbus is obligated to perform.

23. On March 1, 2024, U.S. Senator Charles Schumer sent a letter to the Centers for Medicare & Medicaid Services explaining that a result of the cyberattack: "Hospitals are struggling to process claims, bill patients, and receive electronic payments, leaving them financially vulnerable. Many hospitals are approaching a financial cliff where they will no longer be able to rely on their cash on hand."[2]

24. On March 4, 2024, The American Hospital Associations ("AHA") sent a letter to Congress stating:

> Unfortunately, UnitedHealth Group's efforts to date have not been able to meaningfully mitigate the impact to our field. Workarounds to address prior authorization, as well as claims processing and payment are not universally available and, when they are, can be expensive, time consuming and inefficient to implement. For example, manually typing claims into unique payer portals or sending by fax machine requires additional hours and labor costs, and switching revenue cycle vendors requires hospitals and health systems to pay new vendor fees and can take months to implement properly.[3]

25. In addition, the AHA explained to Congress that the funding assistance program United claims is helpful, is not:

> In addition, UnitedHealth Group's "Temporary Funding Assistance Program" that it stood up as part of its response on March 1 will not come close to meeting the needs of our members as they struggle to meet the financial demands of payroll, supplies and bond covenant requirements, among others.[4]

---

[2] https://www.democrats.senate.gov/imo/media/doc/ces-cmsresponsechangehealthcareoutage3-1- 24pdf.pdf

[3] *See* https://www.aha.org/lettercomment/2024-03-04-aha-urges-congress-provide-support-help-minimize- further-fallout-change-healthcare-attack.

[4] https://www.optum.com/en/business/providers/health-systems/payments-lending-solutions/optum- pay/temporary-funding-assistance.html (explaining Temporary Funding Assistance Program for providers).

26. On March 19, 2024, the AHA again sent a letter to Congress explaining that is had conducted a survey of approximately 1,000 hospitals, concerning the cyberattacks impact, and explained:

> Change Healthcare's downed systems are hampering providers' ability to verify patients' health insurance coverage, process claims and receive payment from many payers, exchange clinical records with other providers, provide cost estimates and bill patients, and, in some instances, access the clinical guidelines used in clinical decision support tools and as part of the prior authorization process. The staggering loss of revenue means that some hospitals and health systems may be unable to pay salaries for clinicians and other members of the care team, acquire necessary medicines and supplies, and pay for mission critical contract work in areas such as physical security, dietary and environmental services. In addition, replacing previously electronic processes with manual processes has often proved ineffective and is adding considerable administrative costs on providers, as well as diverting team members from other tasks.

27. According to AHA's March 2024 survey (titled: "AHA Survey: Change Healthcare Cyberattack Significantly Disrupts Patient Care, Hospitals' Finances") of nearly 1,000 hospitals concerning the cyberattack:

(1)

> "74% of hospitals report direct patient care impact. Nearly 40% report patients having difficulty accessing care because of delays in processing of health plan utilization requirements (e.g. prior authorization)."[5]

(2)

> "94% of hospitals report financial impact, with more than half reporting 'significant or serious' impact. 82% of hospitals report impacts on their cash flow. Of these: More than 33% report impact to more than half of their revenue. Nearly 60% report that the impacts to revenue is $1 million per day of greater. 44% report they expect the negative impact on revenue to continue for 2-4 more months. There is still substantially uncertainty over revenue cycle impacts, with more than 20% currently uncertain of the magnitude of the impacts."[6]

---

[5] https://www.aha.org/system/files/media/file/2024/03/aha-survey-change-healthcare-cyberattack- significantly-disrupts-patient-care-hospitals-finances.pdf

[6] *Id.*

28. On April 16, 2024, the House Energy and Commerce Committee held a hearing entitled "Examining Health Sector Cybersecurity in the Wake of the Change Healthcare Attack." According to a Committee Press Release, "This hearing will give Members the opportunity to hear from industry experts from across the health care system on what more needs to be done to secure patients' sensitive health information and protect our health care sector from disruption."[7]

29. On May 1, 2024, the Senate Finance Committee held a hearing concerning the cyberattack. The only witness was Andrew Witty, CEO of UnitedHealth Group. According to Senator Wyden:

> In the wake of the hack, United essentially disconnected Change from the rest of the health care system. It took weeks for Change to get back online, leaving health care providers in a state of financial bedlam. Doctors and hospitals went weeks delivering services but without getting paid. Insurance companies couldn't reimburse providers. Even today, key functions supporting plans and providers, including sending receipts for services that have been paid and the ability to reimburse patients for their out-of-pocket costs, are not back up and running.
>
> …
>
> Mr. Witty owes Americans an explanation for how a company of UHG's size and importance failed to have multi-factor authentication on a server providing open door access to protected health information, why its recovery plans were so woefully inadequate and how long it will take to finally secure all of its systems.[8]

30. On May 1, 2024, Mr. Witty also testified before the House Energy and Commerce Committee and stated approximately one-third of Americans may have been compromised by the cyberattack and that Change paid a $22 million ransom to hackers.

---

[7] https://energycommerce.house.gov/posts/chairs-rodgers-and-guthrie-announce-health-subcommittee- hearing-on-health-care-cybersecurity.

[8] https://www.finance.senate.gov/imo/media/doc/0501wydenstatement.pdf.

31. In his opening statement to the Committee, Mr. Witty acknowledged "As a result of this malicious cyberattack, patients and providers have experienced disruptions and people are worried about their private health data. To all those impacted, let me be very clear: I am deeply sorry."

32. Given that it is a company in which half of America's medical payments flow, Change needs to maintain the utmost security of its systems. Indeed, Change states on its website that "[w]e implement and maintain organizational, technical, and administrative security measures designed to safeguard the data we process against unauthorized access, destruction, loss, alteration, or misuse."[9] As a sophisticated business entity, making promises that its systems were safe and secure, Change knew it needed to adequately protect those systems. It failed to do so.

33. According to reports, Change allowed its data and systems to be encrypted by the "Blackcat" ransomware gang, affiliated with AlphV. Ransomware attacks encrypt a target's computer systems in a manner that prevents the target from gaining access to their material, unless a ransom is paid in return for the passcode required to decrypt the system. It is a common form of cyberattack, and one that Change should have known it would be threatened with.

34. Defendant Change did not use reasonable security procedures and practices suited to the sensitive information they were maintaining. Worse, it compounded the attack by disconnecting all of its services, even though reports indicate that only certain systems were affected. By disconnecting all services, Change guaranteed that no medical providers could be paid for their services and providers like

[9] https://www.changehealthcare.com/privacy-notice.

Columbus and its payors which relied on Change's systems for authorizations would be unable to obtain such authorizations and therefore enable patients to cycle into Columbus as part of the continuum of care.

35. Given the nature of the healthcare sector, many medical providers, especially hospitals, like the Columbus, are forced to rely on prompt payment of claims in order to operate their businesses and prompt ability to obtain prior authorizations to admit patients and maintain census and occupancy levels required for financial sustainability.

36. Columbus is ordinarily paid by insurance companies to settle their charges for services. Columbus was unable to secure this payment due to Change's system lockout, and thus was denied substantial amounts from the date of the Cyberattack through the date of this complaint.

37. Had Change adequately secured its systems this large amount would have been timely paid, as Columbus had every reason to expect.

CLAIMS FOR RELIEF COUNT I
Negligence

38. Columbus reallege the allegations above as if fully set forth herein.

39. At all times herein relevant, Defendants owed Columbus a duty of care, *inter alia*, to act with reasonable care to secure and safeguard that thei claims and revenue cycle services would be processed on time and for the correct amounts. Defendants took on this obligation and used their computer systems and networks to ensure that proper payments of claims were to be made.

40. Among these duties, Defendants were expected to provide claims processing and revenue cycle services to Columbus using safe and secure computer systems and networks.

41. Defendants owed a duty of care to not subject Columbus to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

42. Defendants knew or should have known of the vulnerabilities of their data security systems and the importance of adequate security. Defendants knew or should have known about numerous well-publicized data breaches.

43. Defendants knew or should have known that their data systems and networks did not adequately safeguard the claims processing and revenue cycle services.

44. Only Defendants were in the position to ensure that their systems and protocols were sufficient to protect Columbus' information.

45. Defendants breached their duties to Columbus by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard the claims processing and revenue cycle services.

46. Because Defendants knew that a breach of their systems could damage numerous individuals, including Columbus, Defendants had a duty to adequately protect their data systems.

47. Columbus' willingness to entrust Defendants with their processing needs was predicated on the understanding that Defendants would take adequate security precautions.

48. Defendants also had independent duties under state and federal laws that required Defendants to reasonably to promptly notify them about the Data Breach.

49. Defendants' willful failure to abide by their duties was wrongful, reckless and/or grossly negligent in light of the foreseeable risks and known threats.

50. As a proximate and foreseeable result of Defendants' grossly negligent conduct, Columbus has suffered damages and are at imminent risk of additional harm and damages.

51. The law further imposes an affirmative duty on Defendants to timely disclose the unauthorized access and failure to be able to process claims corrected or timely.

52. Further, explicitly failing to provide timely and clear notification of the Data Breach to Columbus, Defendants prevented Columbus from taking meaningful, proactive steps to secure processing needs which caused damages to the Hospitals.

53. There is a close causal connection between Defendants' failure to implement security measures to protect Columbus' processing requirements.

54. Defendants' wrongful actions, inactions, and omissions constituted (and continue to constitute) common law negligence.

55. The damages Columbus has suffered (as alleged above) and will continue to suffer were and are the direct and proximate result of Defendants' grossly negligent conduct.

56. Additionally, 15 U.S.C. § 45 (FTC Act, Section 5) prohibits "unfair […] practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect private information like the processing of confidential claims. The FTC publications and orders described above also form part of the basis of Defendants' duty in this regard.

57. Defendants violated 15 U.S.C. § 45 by failing to use reasonable measures

and by not complying with applicable industry standards, as described in detail herein.

COUNT II
Breach of Confidence

58. Columbus reallege the allegations above as if fully set forth herein.

59. During Columbus' interactions with Defendants, Defendants were fully aware of the important and confidential nature of the processing materials that Columbus provided to them.

60. As alleged herein and above, Defendants' relationship with Columbus was governed by promises and expectations that Columbus' claims processing and revenue cycle service materials would be kept in confidence, and would not be accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third parties.

61. Columbus provided its respective claims processing and revenue cycle services to Defendants with the explicit and implicit understandings that Defendants would protect and not permit the materials to be accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third parties.

62. Columbus also provided their claims processing and revenue cycle service materials to Defendants with the explicit and implicit understanding that Defendants would take precautions to protect those materials from unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use, and/or viewing, such as following basic principles of protecting their networks and data systems and make ensure that claim payments related to the materials would be promptly paid and satisfied.

63. Due to Defendants' failure to prevent, detect and avoid the Data Breach from occurring by, *inter alia*, not following best information security practices to secure Columbus' claim processing, Columbus' materials were encumbered by and, not able to be used by in the manner expected.

64. As a direct and proximate cause of Defendants' actions and/or omissions, Columbus suffered damages, as alleged herein.

65. But for Defendants' failure to maintain and protect Columbus' claims processing and revenue cycle services materials in violation of the parties' understanding of confidence, their materials would not have been accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third parties.

66. The injury and harm Columbus suffered and will continue to suffer was the reasonably foreseeable result of Defendants' unauthorized misuse of Columbus' materials. Defendants knew their data systems and protocols for accepting and securing Columbus' materials had security and other vulnerabilities that placed Columbus' materials in jeopardy.

COUNT III
Breach of Implied Contract

67. Columbus reallege the allegations above as if fully set forth herein.

68. Through their course of conduct, Defendants, Columbus entered into implied contracts for Defendants to implement data security and data processing functions adequate to safeguard and protect Columbus' claims processing and revenue cycle services materials.

69. Defendants required Columbus to provide and entrust their claims

processing and revenue cycle services materials as a condition of obtaining Defendants' services.

70. Defendants solicited and invited Columbus to provide their claims processing and revenue cycle service materials as part of Defendants' regular business practices. Columbus accepted Defendants' offers and provided their claim processing materials to Defendant.

71. Columbus provided and entrusted their claims processing and revenue cycle services materials to Defendant. In so doing, Columbus entered into implied contracts with Defendants by which Defendants agreed to ensure that the Columbus' processing materials would not be defective or compromised.

72. A meeting of the minds occurred when Columbus agreed to, and did, provide their claims processing and revenue cycle services materials to Defendant, in exchange for, amongst other things, the protection of their materials.

73. Columbus fully performed their obligations under the implied contracts with Defendant.

74. Defendants' breaches caused economic and non-economic harm.

COUNT IV
Breach of the Implied Covenant of Good Faith and Fair Dealing

75. Columbus reallege the allegations above as if fully set forth herein.

76. Contracts have an implied covenant of good faith and fair dealing. This implied covenant is an independent duty and may be breached even when there is no breach of a contract's actual and/or express terms.

77. Columbus has complied with and performed all conditions of their contracts with Defendants.

78. Defendants breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices and to process claims and services in a timely and safe manner as a result of the Data Breach.

79. Defendants knew or should have known of the vulnerabilities of the systems that were exploited in the Data Breach.

80. Defendants acted in bad faith and/or with malicious motive in denying Columbus the full benefit of their bargains as originally intended by the parties, thereby causing them injury in an amount to be determined at trial.

COUNT V
Breach of Fiduciary Duty

81. Columbus reallege the allegations above as if fully set forth herein.

82. In light of the special relationship between Defendants and Columbus, whereby Defendants became the guardian of Columbus' claim processing materials, Defendants became a fiduciary by their undertaking and guardianship of the materials to act primarily for Columbus.

83. Defendants have a fiduciary duty to act for the benefit of Columbus upon matters within the scope of their relationship with Columbus—in particular, to keep their claims processing and revenue cycle service materials secure.

84. Defendants breached their fiduciary duties to Columbus by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period of time.

85. Defendants breached their fiduciary duties to Columbus by failing to encrypt and otherwise protect the integrity of the systems containing Columbus' claims processing and revenue cycle service materials.

86. Defendants breached their fiduciary duties to Columbus by failing to timely notify and/or warn the Columbus of the Data Breach.

87. As a direct and proximate result of Defendants' breaches of their fiduciary duties, Columbus suffered and will continue to suffer injuries.

COUNT VI
Unjust Enrichment

88. Columbus reallege the allegations above as if fully set forth herein. This Count is pleaded in the alternative to the Breach of Contract Count above.

89. Upon information and belief, Defendants fund their data-security measures entirely from their general revenue, including payments made by or on behalf of Columbus.

90. As such, a portion of the payments made by or on behalf of Columbus is to be used to provide a reasonable level of data security, and the amount of each payment allocated to data security is known to Defendants.

91. Columbus conferred a monetary benefit to Defendant. Specifically, they purchased goods and services from Defendants and/or their agents and provided Defendants with their claims processing and revenue cycle service materials. In exchange, Columbus should have received from Defendants the goods and services that were the subject of the transaction and have their processing and service materials protected with adequate data security.

92. Defendants knew that Columbus conferred a benefit which Defendants accepted. Defendants profited from these transactions and used the claims processing and revenue cycle service materials of Columbus for business purposes.

93. Defendants enriched themselves by saving the costs it reasonably should

have expended in data-security measures to secure Columbus' claims processing materials. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendants instead calculated to increase their own profits at the expense of Columbus.

94. Under the principles of equity and good conscience, Defendants should not be permitted to retain the money belonging to Columbus, because Defendants failed to implement appropriate data management and security measures mandated by industry standards.

95. If Columbus knew that Defendants had not reasonably secured their claims processing materials, they would have avoided transacting business with Defendants and to those providers that Defendants did business with, which provided services to Columbus.

96. As a direct and proximate result of Defendants' conduct, Columbus suffered and will continue to suffer other forms of injury and/or harm.

97. Defendants should be compelled to disgorge into a common fund or constructive trust, for the benefit of Columbus, proceeds that it unjustly received from them. In the alternative, Defendants should be compelled to refund the amounts that the Columbus overpaid for Defendants' services.

PRAYER FOR RELIEF

WHEREFORE, Columbus, respectfully requests that the Court enter judgment in their favor and for the following specific relief against Defendants as follows:

1. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

2. That the Court enjoin Defendants, ordering them to cease and desist from similar

unlawful activities;

3. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein and from refusing to issue prompt, complete, and accurate disclosures to Columbus.

4. For injunctive relief requested by Columbus, including but not limited to injunctive and other equitable relief as is necessary to protect the interests of Columbus;

5. For prejudgment interest on all amounts awarded, at the prevailing legal rate;

6. For an award of attorney's fees, costs, and litigation expenses, as allowed by law; and

7. For all other Orders, findings and determinations identified and sought in this Complaint.

JURY DEMAND

Columbus demands a trial by jury for all issues triable by jury.

CERTIFICATION PURSUANT TO LOCAL CIVIL RULE 11.2 AND CERTIFICATION OF SERVICE

Pursuant to Local Civil Rule 11.2, the Defendant, by their attorneys, The Agresta Firm, P.C., states that the matter in controversy is the subject of a Multi District Litigation involving the same facts entitled Change Healthcare, Inc. Customer Data Security Breach Litigation, MDL No. 3108 and this matter should be appropriately joined into the Multi District Litigation. Defendant further certifies that this pleading was served within the time period allowed under the rules and appropriate court orders.

s/ Robert A. Agresta
Robert A. Agresta, Esq. (RA0218)
THE AGRESTA FIRM, P.C.
24 Grand Avenue
Englewood, New Jersey 07631
(201) 399-6888
robert.agresta@agrestalaw.com
Attorneys for Columbus LTACH, LLC

Dated: December 26, 2024